UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Marc Opperman, *et al*.,	§	
for themselves all others	§	
similarly situated,	§	
Plaintiffs,	§	Case No. 1:12-00219-SS
vs.	§	
	§	
Path, Inc., *et al.,*	§	
Defendants.	§	

PLAINTIFFS' RESPONSE TO DEFENDANT APPLE'S
MOTION TO DISMISS UNDER 12(B)(6) AND FOR CDA IMMUNITY

Plaintiffs respectfully request that this Court deny Apple's Motion to dismiss Plaintiffs' Second Amended Complaint [Dkt # 103] ("SAC") under Rule 12(b)(6) because Plaintiffs properly stated valid claims against Apple.

I. Introduction

Apple moves to dismiss Plaintiffs claims for the following reasons under Rule 12(b)(6): (1) despite their numerous representations to the contrary, Apple has disclaimed any duty to protect its customers' privacy, even when they know they know the Apps they are selling and providing are without authorization acquiring and uploading those customers' iDevice address book contents for commercial gain; (2) Plaintiffs have failed to plead that Apple received a benefit from its participation in the thefts of its customers' iDevice address books; and (3) aiding and abetting is not recognized in Texas; and (4) Plaintiffs fail to state a valid claim under RICO against it.

The court should reject each of these arguments.

Apple's attempts to disclaim all duties to protect Plaintiffs' and consumers' privacy from the malicious apps that captured their private iDevice address books is flawed.[1] It has repeatedly – in public to the FCC no less, not in private as Apple claims – asserted that it rigorously reviews the Apps it provides to consumers and that it does so to protect its customers' privacy. Thus, it has voluntarily assumed a duty to review its apps and to protect its users' privacy, and must do so reasonably. As pled in the SAC, it did not, which proximately caused damage to Plaintiffs and their property.

Plaintiffs have also alleged negligence claims concerning the iDevice itself, namely that Apple negligently designed the iDevice and failed to warn iDevice owners of the security flaw in the iDevice. These are duties they appear to have not disclaims, at least not in documents provided to the Court as of yet.

Contrary to their representations to the Court, Plaintiffs SAC does allege that Apple knew that its co-defendants were surreptitiously stealing Plaintiffs' private iDevice address book materials, and that the silent thefts were occurring specifically because their iDevice had a security flaw. In fact, Apple appears to have assisted the Apps exploit its security flaw. SAC ¶¶ 1-7, 56-83. And not only did Apple know the iDevices were flawed, Apple chose not to warn consumers that their amassed address book contacts would be or were being taken – even after researchers notified them that the Gowalla app was secretly harvesting their users' iDevice address books. In fact, as alleged in the SAC, Apple did far more than fail to mind the store, the Apps in question were partly made by Apple and contain Apple components and digital certificates. Per the SAC, Apple worked in concert with the co-defendants to place spyware on Plaintiffs' iDevices.. Thus, Plaintiffs have stated valid claims against Apple for negligence, for

[1] For starters, Apple's recently submitted privacy policy and terms of service are not mentioned in Plaintiffs' SAC. Therefore, they should not be considered in a motion to dismiss.

substantially assisting or working in concert with the various App Developer Defendants, and for RICO.

Finally, contrary to its motion, Apple received significant monies from the app developer program and from downloads of Rovio's Angry Birds and ZeptoLab's Cut the Rope. It also received significant financial benefits through the marketing of the other defendants' "free" Apps. As the conduct on which those gains were made was wrongful, Plaintiffs have stated a claim for unjust enrichment.

Accordingly, the Court should deny Apple's motion to dismiss in its entirety.

II. Background[2]

Plaintiffs are fourteen individual consumers who each created and own[3] their own valuable, private proprietary iDevice address books,[4] which they regularly used with their iDevices[5] to contact and communicate with their own social networks. SAC ¶¶ 2. 8-28, 89-92, 92, 129, 300, 306, 310, 369. Plaintiffs explicitly state that such address books have intrinsic, extrinsic and commercial value and are not generally known to others. SAC ¶¶ 77, 78, 315-16 Plaintiffs allege that Apple, Inc. ("Apple") and its co-defendants' products and actions directly injured each of the plaintiffs in this action. SAC ¶¶ 7, 76-83.

---

[2] "The court must take the allegations of the complaint as true and draw all inferences in the plaintiff's favor." *Armstrong v. Tygart*, No. A-12-CA-606-SS (W.D. Tex. Aug. 20, 2012) (citing *Saraw P'ship v. United States*, 67 F.3d 567, 569 (5th Cir. 1995).

[3] *See* SAC ¶ 129 (noting that Apple has told participants in its app developer program that "the Address Book database is ultimately owned by the user") (emphasis added).

[4] Per the Fifth Circuit, cell phone address books are private. *See United States v. Zavala*, 541 F.3d 562, 577 (5th Cir. 2008) ("[C]ell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber names. Zavala [the cell phone owner] had a reasonable expectation of privacy regarding this information."); *United States v. Wurie*, 612 F. Supp.2d 104, 109 (D. Mass. 2009) (observing that it "seems indisputable that a person has a subjective expectation of privacy in the contents of his or her cell phone").

[5] The term "iDevices" includes iPhones, iPads and iPod touches made by Apple, Inc. ("Apple").

First, Apple sold these plaintiffs iDevices marketed as safe, secure and useful to, in part, maintain and manage their owners' private address books. SAC ¶¶ 58, 60, 83-88, 125-132.[6] Apple, however, knew that they were not; iDevice address books were instead insecure and, it turns out, remotely uploadable. SAC ¶¶ 69, 71, 136, 138-41, 146-49, 161. As a result, Plaintiffs overpaid for their iDevices, SAC ¶¶ 83, and their iDevice address books were repeatedly poached.[7] SAC ¶¶ 2, 59, 65-66, 138-271. Plaintiffs sued Apple to recover the amount they overpaid for and the cost to fix their damaged iDevices, SAC ¶¶ 76, 82-83, 136, 418, as well as for the foreseeable damages they suffered as a consequence of their private iDevice address books being intentionally or negligently left insecure by Apple and, as a direct result, being poached by others. *Id.*; SAC ¶¶ 3, 329-32.

Second, the poachers and Apple worked together closely. SAC ¶¶ 105-114. Had they not, the poaching could not have occurred.[8] SAC ¶¶ 105-08, 114. The poachers "develop[ed]"

---

[6] Long-time Apple CEO Steve Jobs repeatedly announced that apps from Apple's "curated" App Store would not do exactly what the apps here did—invade users' privacy, steal their private information and trash their device's battery. SAC ¶¶ 127-31.

[7] For brevity's sake, the terms "poached" or "took" generally convey the myriad terms used in the SAC (e.g., appropriated, converted, trespassed upon, stole, etc.) to describe how defendants purloined Plaintiffs' private, proprietary iDevice address books.

[8] Apple requires companies to join Apple's app developer program and execute Apple's standard iPhone Developer Program License Agreement ("IDPLA") [Dkt # 134-6] and iPhone SDK Agreement ("SDK") [Dkt # 134-7]before it will test, approve, release or sell apps to iDevice consumers via its App Store. SAC ¶¶ 98, 105, 108-11; Apple IDPLA (Ex. 5) at pp. 1, 6. Thus, the co-defendant poachers necessarily were in Apple's app developer program, had agreed to Apple's IDPLA and SDK, and developed the apps "using this Apple software." *Id*. In another lawsuit, Apple described its multi-faceted relationship with its app co-defendants as follows:

> Apple designs and offers a comprehensive ecosystem of technologies and services that enable the delivery of software applications (or "Apps") such as games, tools, and educational services on Apple devices such as the Mac, iPhone, iPad, and iPod Touch. In order to access Apple hardware and software, the Developers use Apple application program interfaces ("APIs"), Apple software development kits ("SDKs"), and Apple's operating system ("iOS"). Together, these Apple products and services permit the Developers to interact with Apple end users through the App Store, where Developer Apps can be purchased or upgraded. Apple also provides a comprehensive set of Apple hosting, marketing, sales, agency and delivery services that allow Developers to provide Apps to millions of Apple end users. In return for Apple's provision of these products and services to the Developers, the Developers agree to pay Apple a percentage of their sales made using Apple's products and services.

apps containing Apple components using Apple tools,[9] SAC ¶¶ 110-11, paid to be in and went through Apple's developer program, SAC ¶¶ 105-08, contractually retained and used Apple as their marketing, sales and distribution agent (amongst other roles),[10] SAC ¶¶ 109-10, and relied on Apple exclusively to bless and digitally-activate their apps in order to access the captive iDevice market controlled by Apple and its iDevice-integrated App Store.[11] SAC ¶¶ 94-108. This occurred before Apple sold or offered the product to consumers. With Apple, they jointly made, tested, marketed, distributed and sold or provided to each plaintiff several superficially-useful but, in actuality, harmful iDevice-compatible apps that, part, poached iDevice address books. SAC ¶¶ 2, 66-75, 95-123, 133-35, 138, 147, 175, 197, 205, 215, 225, 231, 238, 246, 260, 410-414.

Unbeknownst to Plaintiffs and without prior warning or permission, SAC ¶¶ 152, 155, 160, 187-88, 199, 207, 218, 222, 239-40, 248, 262-63, 267, defendants' apps caused Plaintiffs' iDevices to transmit and upload Plaintiffs' private iDevice address books to, and disseminate those address books over, the internet, amounting to an electronic disclosure. SAC ¶¶ 5, 12, 56-57, 64-68, 154, 186, 201, 208, 220, 228, 235, 358. Apple's co-defendants captured the transmissions,[12] SAC ¶¶ 66, 156, 162, 181, 212, 220, 229, 236, 241, 251, 264, thereby obtaining

---

Apple Motion to Intervene on 7/9/11 (Exhibit 7) at p. 7, *Lodsys, LLC v. Combay, Inc*., No. 2:11-cv-0272 (E.D. Tex.).

[9] Apple Post, *Apple Answers the FCC's Questions*, available at < http://www.apple.com/hotnews/apple-answers-fcc-questions/> (attached as Exhibit 3) ("We provide every developer with the same software that we use to create our own iPhone applications."); SAC ¶¶ 118.

[10] Apple IDPLA (Ex. 5) at p. 23 (appointing Apple to solicit orders for, host, and market iDevice apps for companies and contracting to "appoint Apple as your worldwide agent for the delivery of the Licensed Applications to end-users . . . in Apple's own name, through one or more App Stores, but for You and on Your behalf").

[11] Apple SDK (Ex. 6) at p. 2, ¶ 2.2 ("Applications must be approved and signed with an Apple-issued certificate. . .. Apple reserves the right to approve or withhold approval and signing of any application at its sole discretion.").

[12] Having not been informed that the iDevices they owned were making these transmissions, SAC ¶¶ 59, 67-68, 72, Plaintiffs could not have intended the defendants to receive them or their content. SAC ¶¶ 399.

for their own competitive business use without compensation to Plaintiffs (and, Plaintiffs' fear, for further disclosure or re-sale, SAC ¶¶ 265, 390, 408-09, 426, 436) their formerly-private address books without expending the efforts that went toward creating them. SAC ¶¶ 196, 300-03, 212, 241, 251. Half of the defendants publicly admitted doing so and two publicly apologized. SAC ¶¶ 6, 61-62, 182-83, 202, 210, 235. Apple, who facilitated, encouraged and enabled their co-defendants' conduct, SAC ¶¶ 3, 4, 7, 58, 98, 103, 410-14, subsequently blamed their co-defendants, telling the press that their address book transgressions had violated Apple's policies. SAC ¶¶ 63.

For quite some time, Apple knew it was activating and providing consumers with address-book-poaching apps that impeded and diminished consumers' iDevices and exposed them and their address books to harm.[13] SAC ¶¶ 3, 58, 71, 105, 109, 114, 118, 136, 138-63, 352.

---

[13] Plaintiffs need not marshal their evidence to prove their claims at this stage, as Apple implies. Realistically, they cannot. Pertinent information, like Apple's precise knowledge about each app, is in defendants' hands and unavailable to Plaintiffs before discovery. Plaintiffs, however, specifically provided a good faith basis for their "knowledge" allegation, pointing to concrete evidence indicating Apple knew it issued harmful address-book-poaching apps in the past, SAC ¶¶ 3, 71, 136-165 (noting reports about the *Aurora Feint*, *Kik Messenger* and *Gowalla* apps), and to an indirect admission by Apple showing that it knew in advance it was doing so for the other apps in suit. Specifically, from 2009 to today, Apple has kept publicly posted on its website an open letter it sent the Federal Communications Commission regarding Apple's direct visibility into each and every iDevice app, wherein Apple says that it:

> [has] an approval process that **reviews every application** submitted to Apple for the App Store in order to protect consumer privacy[.] . . . **Apple alone makes the final decisions to approve or not approve iPhone applications** . . . Apple developed a **comprehensive review process** that **looks at every iPhone application** that is submitted to Apple. Applications and marketing text are submitted through a web interface. Submitted applications undergo a **rigorous review process**.

Apple Post, *Apple Answers the FCC's Questions* (Ex. 3); SAC ¶¶ 118. So according to Apple, it "rigorous[ly]" and "comprehensive[ly]" reviewed its co-defendants' address-book-poaching apps in advance of inflicting them upon the unsuspecting consumer marketplace. As individuals with fewer resources and less technical sophistication than Apple detected (and first reported on) these apps' harmful address-book-poaching functions using a simple, free, readily-available *mitmproxy* tool, *see* SAC ¶¶ 5, 61, 64, 148, 177-79, 196, 219, 249; *Mitmproxy "Download" web page*, available at <www.mitmproxy.org> (attached as Exhibit 4), the obvious inference is that Apple did, too, during its "comprehensive" and "rigorous review" of each app. The alternatives, that Apple either (a) lied to the FCC and used, at most, an inadequate review process, or (b) reviewed but repeatedly failed to notice that any of a dozen or so of its most popular iDevice apps had embedded address-book-poaching functions, are equally bad. Nevertheless, Apple's letter—from which the Court must infer that Apple knew about each app's harmful, complained-of functions in advance of its release—combined with Apple's published statement that address-book-poaching functions violate Apple's policies, SAC ¶¶ 63, effectively prohibit dismissal or summary judgment of

Nevertheless, Apple failed to take reasonable steps (like modifying its iDevices, improving its testing/vetting/selection process, or mandating address book "hashing," a blind-matching method that would not disclose the raw address book to anyone) to inhibit the recurrence of additional harmful app releases. SAC ¶¶ 3, 67, 71. Apple did not warn consumers about the specific Apps that were poaching Plaintiffs' private iDeivice address books.

Plaintiffs therefore also sued Apple for materially assisting the poachers and facilitating their conduct (and sought to hold Apple jointly liable for the harms discussed above), SAC ¶¶ 7, 69, 72, 410-14, and for recklessly or negligently failing to initiate appropriate app development- and/or review-protocols to catch and cull address-book-poaching apps while they had the app product and before endorsing it to the public. SAC ¶¶ 58, 71-72, 164, 329. By its failures, Apple chose and brought iDevice address-book-poaching apps to market knowing they were flawed (or in reckless disregard of those evident flaws) and in contravention of Apple's own policies and industry standards. SAC ¶¶ 99, 109, 114, 117-32, 149, 164.

Finally, Apple's role in creating and releasing these address-book-poaching apps was more than just not minding the App Store. SAC ¶¶ 98, 110-11, 133-35, 410-14. These apps incorporate Apple guidance and include Apple components and certificates. SAC ¶¶ 102-03, 112. As alleged in the SAC, Apple repeatedly worked actively with its co-defendants to knowingly make, put out, and distribute to a network of iDevices via the App Store hierarchy these faulty, harmful, noncompliant address-book-poaching app products. SAC ¶¶ 103, 106, 133-35, 142-45. Apple did not unwittingly assist the poachers; in view of its admissions it likely

---

many claims in suit. Perhaps that is why Apple's motions now suggests that Apple had no duty to protect consumers or their address books, despite telling the government in 2009 and continuing to tell the public via its posted FCC letter that it would do so.

conspired with them,[14] SAC ¶¶ 133-35, 142-45, received business benefits from placing these apps on millions of consumers' iDevices, SAC ¶¶ 133-5, 361-68, and continues to provide cover for them to this day.[15] SAC ¶¶ 3, 4, 67, 71-72. Apple and each of its co-defendants, it appears, joined to form a malware-spyware distribution/address book contacts acquisition ring, SAC ¶¶ 7, 58, 75, 102-03., 112, 114, 133-35, 362-65; wherein Apple and the co-defendants collaboratively and repeatedly used the wires and the internet[16] (i.e., a network), *e.g.,* SAC ¶¶ 175, 357-59, 391-404, and the networked on- and off-device App Store hierarchy (another network/enterprise), SAC ¶¶ 86, 93-99, 106, 197, 205, 215, 225, 231, 238, 246-47, to distribute their Trojan-horse malware to millions of networked iDevices, turning recipients' iDevices into prohibited bots[17] which, in essence, electronically eavesdropped on their owners and (again via the internet and the airwaves) disclosed their associates to others and took and reported back to each respective co-defendant the iDevice owners' private, proprietary address books, SAC ¶¶ 56-59, 80, 186, 200, 208, 219-20, 228, 235, 240, 249, 253, 264, which defendants then used and integrated without consent into their own networks. SAC ¶¶ 79, 156, 162, 186, 201, 208, 220, 228, 236, 240, 249,-51, 265-66, 418-420, 425, 427.

---

[14] *Id.* It would stretch the bounds of incredulity to imagine twelve different sophisticated tech companies independently sneaking apps past Apple's "comprehensive review" to simultaneously embark on schemes to poach iDevice address books using the wires. More plausible (and reasonably inferable) is that Apple green-lighted this conduct. *See supra*, n. 14. These pled facts and reasonable inferences, alone, should permit Plaintiffs to move forward and discover from Defendants who knew what and when, even on claims going to the defendants' most egregiously conduct. Moreover, Apple appears to have an ownership stake in co-defendant Path, Inc. and played a hands-on advisory role in the creation of the Path app through its participation in the iFund venture fund and mentoring program. SAC ¶¶ 168.

[15] As noted, a $99 payment ($50M annually in the aggregate to Apple) for participation in Apple's iOS developer program is apparently all it takes for an app company to come within Apple's self-imposed, ongoing sphere of protection from consumer claims about harmful apps. SAC ¶¶ 98.

[16] *See United States v. Faulkner*, 17 F.3d 745, 771 (5th Cir. 1994) (noting the essential elements of wire fraud to be: (1) a scheme to defraud and (2) the use of, or causing the use of, interstate wire communications to execute the scheme), *cert. denied*, 115 S.Ct. 193 (1995).

[17] TEX. BUS. COM. CODE § 324.054-.055 (prohibiting spyware, computer "bots" or "zombies," and unauthorized use of another's computer or transmission of another's computer data).

III. Argument

A. Legal Standard

On a motion to dismiss under Rule 12(b)(6), the Court must accept all well pleaded facts as true and view them in the light most favorable to the plaintiff.[18] The issue is not whether the plaintiffs will prevail at trial (two Defendants,' prior public apologies for taking customers' iDevice address books suggests Plaintiffs should), but rather whether plaintiffs are entitled to pursue their complaint at all and offer evidence in support of their claims.[19] Thus, Rule 12(b)(6) motions are disfavored and should rarely be granted.[20] Indeed, dismissal or judgment must not be granted unless it appears beyond doubt that plaintiffs can prove no set of facts in support of their claims that might entitle them to relief.[21]

A party's complaint need merely be plausible on its face, offer more than labels and conclusions, and provide some factual basis in support of its claim.[22] Plaintiffs' SAC does more than that here. Moreover, as plaintiffs are unlikely before discovery to have access to defendants' specific records, policies or protocols or only into their non-public activities or the internal workings of their products (more so in a technology case like this), only "minimal factual allegations should be required at the motion to dismiss stage."[23]

Also, if a defendant continually refers to and relies on matters outside the pleadings in its motion to dismiss, the motion should be treated as one for summary judgment under Rule 56(d),

[18] *Baker v. Putnal,* 75 F. 3d 190, 196 (5th Cir. 1996).
[19] *Doe v. Hillsborough Indep. Sch. Dist.*, 81 F.3d 1395, 1401 (5th Cir. 1996).
[20] *Bernal v. Freeport-McMoran, Inc.,* 197 F.3d 161, 164 (5th Cir. 1999). (emphasis added)
[21] *Young v. City of Houston*, 471 Fed. Appx. 389, 389-390 (5th Cir. 2012); *Morin v. Caire*, 77 F. 3d 116, 120 (5th Cir. 1996).
[22] *Ashcroft v. Iqbal* 129 S. Ct. 1937, 1949 (2009).
[23] *Thomas v. City of Galveston*, 800 F. Supp. 2d 826, 842 (S.D. Tex 2011).

not under Rule 12, and consideration of it deferred until the plaintiff has had adequate opportunity for discovery.[24] [25]

B. Plaintiffs state a valid RICO claim against Apple.

Plaintiffs' "RICO" claims against Apple are straightforward. In a nutshell, Plaintiffs allege a ring consisting of Apple and the other defendants who worked with Apple and issued an app that Apple knew[26] was spyware before delivering it. With respect to those parties, Apple and its co-defendants committed evident § 1962(c) violations by repeatedly distributing spyware over the wires to consumers' iDevices which, in turn, repeatedly and impermissibly acquired consumers' private iDevice address books (i.e., property) and uploaded them over the wires via the internet to the respective RICO defendants. SAC ¶¶356-68.

RICO's § 1962(c) prohibits, among other things, those "associated" with a legitimate business organization from regularly using the business for any illegal "racketeering" acts listed in § 1961.[27] Two types of acts listed in § 1961 are wire fraud under 18 U.S.C. § 1343 and transportation of stolen property under 18 U.S.C. § 2314 cl. 2.

Here, the defendants[28] associated with and who participate in Apple's app developer program and make use of Apple's networked and iDevice-integrated App Store hierarchy

[24] Fed. R. Civ. P. 12(d); *Darklak v. Bobear*, 814 F. 2d 1055, 1064 (5th Cir. 1987).

[25] Moreover, Apple also violated industry standard set by Google and Amazon, further evidence of its lack of good faith. SAC ¶¶__.

[26] Apple claims to rigorously review every app before activating it with a digital certificate and was informed by others about the malicious features of at least two apps that continued to deliver to the public. SAC ¶¶ 58, 98, 103, 105, 106, 114-16, 127-130, 148, 161, 364. Thus, the reasonable inference is that Apple knew how each App functioned.

[27] 18 U.S.C. § 1962(c) ("It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt."); 18 U.S.C. § 1961(1) (listing the "predicate acts" subject to RICO); *U.S. v. Casamayor*, 837 F.2d 1509 (11th Cir. 1989) (convicting former sheriffs under § 1962(c) for running a cocaine distribution ring and protection racket through the Key West Sheriff's Department).

essentially operated and participated in a spyware manufacture & distribution ring and complimentary electronic iDevice address book piracy operation via the app developer program and App Store organizational hierarchy. SAC ¶¶ 93-116, 357-60. The defendants routinely and without authorization made, sold and distributed over the wires spyware and using the wires obtained and transported in interstate commerce stolen iDevice address book properties.[29] In doing so, they have repeatedly violated § 1343 and § 2314.

The SAC describes the RICO defendants' recurring manufacture and distribution of spyware and illegal acquisition of Plaintiffs' and other consumers' private, proprietary iDevice address book properties. SAC ¶¶ 146-271, 357-60. Consequently, Plaintiffs have been directly harmed as a result of the RICO defendants' racketeering activities. SAC ¶ 367. As the SAC alleges, these RICO defendants repeatedly engaged in these actions over a period of indefinite length, of which only they know the precise timeframe. *See supra.*

Thus, Apple and its RICO defendants' illicit activities fall squarely within and are actionable under § 1962(c) because they participated in the conduct of the app developer program and App Store heirachchy's structured organization's affairs through a "pattern" of wire fraud and transported stolen property that resulted in direct harm to Plaintiffs. SAC ¶¶ 361-365. Because the RICO defendants collaborated with Apple and conspired to engage in these acts, *Id.;* SAC ¶¶ 243-71, they violated § 1962(d) as well.[30]

While the spyware-related harms or value of the property stolen may be debatable, the RICO defendants actions nonetheless are the sort of conduct that § 1962 was meant to remedy.[31]

---

[29] *See also* SAC at ¶¶ 357-60. The apps are delivered and sold via the App Store and via the internet. SAC ¶¶ 84-115.

[30] 18 U.S.C. § 1962(d) ("It shall be unlawful for any person to conspire to violate any of the provisions of subsection (a), (b), or (c) of this section.").

[31] Plaintiffs' RICO claims are based on the defendants' distribution of spyware and appropriation of iDevice address book properties via the wires in violation of 18 U.S.C. §§ 1343 and 2314. Ample public proof exists of defendants'

Provided Apple knew the harmful capability, as is alleged, of any of its co-defendants' apps,[32] then a broad-based conspiracy to distribute malware and harvest iDevice contacts existed that involved it, too.

"RICO claims under §1962 have three common elements: '(1) a person who engages in (2) a pattern of racketeering activity, (3) connected to the acquisition, establishment, conduct or control of an enterprise.' " *Abraham v. Singh*, 480 F. 3d 351, 355 (5th Cir. 2007) (quoting *Word of Faith Outreach Ctr. Church, Inc. v. Sawyer*, 90 F. 3d. 118, 122 (5th Cir. 1996)). The second element – a "pattern of racketeering activity" –consists of two components: (1) predicate acts (the racketeering activity) and (2) a pattern of such acts. *In re Burzynski*, 989 F. 2d 733, 742 (5th Cir. 1993). A "pattern of such acts" means that: (1) the predicate acts are related to each other, and (2) they either constituted or threaten long-term criminal activity. *Id; see also St. Paul Mercury Ins. Co. v. Williamson,* 224 F. 3d 425, 441 (5th Cir. 2000). A plaintiff must also plead sufficient facts to comprise a violation of the substantive RICO subsections, §§1962 (a)-(d), the plaintiff acuses a defendant of violating. *Abraham* 480 F. 3d at 355.

Here, Apple's RICO liability is evident in the pleadings.

A. The RICO defendants' culpability on the "predicate acts" of wire fraud and transporting stolen property is evident

Wire fraud and transportation of stolen property under 18 U.S.C. §§ 1343 and 2314 are "predicate acts" under the *RICO* statute.[33]

---

conduct via their creation of spyware that Apple publicly stated was in violation of policies, SAC ¶¶ 63, and that apologies were issued upon, SAC ¶ 62. Certain defendants' publicly admitted possession of consumers' iDevice address book records and Apple explaining its visibility into each defendants' app and its features and operations via the app developer program and testing and validation procedures. *See, e.g.,* SAC ¶¶ 3, 58, 98-99, 105-116, 1 36, 148, 161. When, as here, such activities are conducted via an organized structure in a repeated and ongoing fashion, they are ordinarily deemed to be *RICO* violations. 18 U.S.C. §1962(c).

[32] Contrary to Apple's motion, it not only rigorously reviewed each app for issues concerning privacy, it was specifically told Gowalla was misappropriating itscustomers' address books. Contrary to its motion, it did not remedy the issue – indicating that it condoned and, in all likelihood, already knew this was occurring.

Apple or defendants' activities—use of the wires and malware to, without asking, poach Plaintiffs' private proprietary iDevice address books—unquestionably constitutes the predicate act of wire fraud[34] under the Supreme Court's *Carpenter* opinion,

> [T]he mail fraud statute [ ] "had its origin in the desire to protect individual property rights." Here, the object of the scheme was to take the Journal's confidential business information - the publication schedule and contents of the "Heard" column - and its intangible nature does not make it any less "property" protected by the mail and wire fraud statutes. McNally did not limit the scope of 1341 to tangible as distinguished from intangible property rights. . . . Petitioners cannot successfully contend . . . that a scheme to defraud requires a monetary loss, such as giving the information to a competitor; ***it is sufficient that the Journal has been deprived of its right to exclusive use of the information***, for exclusivity is an important aspect of confidential business information and most private property for that matter,

see Carpenter v. United States, 484 U.S. 19, 25-27 (1987) (citations omitted and emphasis added), and necessarily involved transportation in interstate commerce of stolen property (i.e., the poached private address books).[35]

---

[33] *See* 18 U.S.C. § 1961(1)(B) ("As used in this chapter[,] 'racketeering activity' means . . . any act which is indictable under any of the following provisions of title 18, United States Code: . . . [including] section 1343 [and] section 2314

[34] 18 U.S.C. § 1343 ("Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both."). *See Carpenter*, 484 U.S. at 27 ("[T]he words 'to defraud' in the mail fraud statute have the 'common understanding' of ``wronging one in his property rights by dishonest methods or schemes,' and `usually signify the deprivation of something of value by trick, deceit, chicane or overreaching.'"') (citations omitted).

[35] 18 U.S.C. § 2314 ("Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud; or Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transports or causes to be transported, . . . in interstate or foreign commerce in the execution or concealment of a scheme or artifice to defraud that person or those persons of money or property having a value of $5,000 or more . . . Shall be fined under this title or imprisoned not more than ten years, or both.") *See also Carpenter*, 484 U.S. at 27; SAC ¶¶ 129, 359 (alleging the aggregate value of the poached address book properties to exceed $5,000.00 a defendant).

Thus, the RICO defendants clearly engaged in multiple distinct but related wire fraud and stolen property transport transactions involving Plaintiffs' iDevice address book properties, which far exceeds RICO's underlying requirement of two predicate acts.[36]

B. The RICO Defendants regularly and routinely distributed spyware and transported back stolen iDevice address book properties via the wires for their own commercial benefit

Plaintiffs sought to recover for the harms they suffered resulting from multiple, enterprise-based conspiracies, including damages inflicted upon their iDevices and iDevice address books discussed above as well as the return of or restitution for their purloined private proprietary iDevice address book materials. SAC ¶¶ 355-68, 417-29, 436-38.

While any one incident of spyware-related wire fraud or transport of stolen iDevice address book property in isolation may not seem overly significant, cumulatively across these Defendants' app user bases they amount to not just a pattern of racketeering activity, but to a clear picture of the RICO defendants' regular, day-to-day business practices wherein they routinely and without a second thought feel free to damage and take others' property via the wires. Thus, this clearly amounted to a continuous, ongoing pattern that fits neatly within the confines of the RICO statutes.[37] Indeed, the RICO defendants' pattern of conduct—repetitive,

---

[36] "A 'pattern of racketeering activity' requires at least two predicate acts." *Trevino v. Pechero*, 592 F.Supp.2d 939, 939-40 (S.D. Tex. 2008). Any two separate but related acts are sufficient. *Id*. at 945 ("[the allegations show] two separate events and thus two occasions of attempted extortion and two predicate acts under RICO").

[37] In *Word of Faith World Community Outreach Center Church*, the Fifth Circuit specifically reiterated that,

> To establish a pattern of racketeering activity, the Supreme Court explained in *H.J. Inc. v. Northwestern Bell Telephone, Co.* 492 U.S. 229, 109 S.Ct. 2893 (1989), that a plaintiff "must show that the racketeering predicates are related, and that they amount to or pose a threat of continued criminal activity." The element of relatedness is established if the acts have the "same or similar purposes, results, participants, victims, or methods of commission." To establish continuity, plaintiffs must prove "continuity of racketeering activity, or its threat." This may be shown by either a closed period of repeated conduct, or an open-ended period of conduct that "by its nature projects into the future with a threat of repetition." A closed period of conduct may be demonstrated "by proving a series of related predicates extending over a substantial period of time." An open period of conduct involves the establishment of "a threat of continued racketeering activity." This may be shown where there exists a "specific threat of repetition extending

collaborative, spyware-related piracy—is a perfect example of activity that Congress tried to curtail by making wire fraud a RICO predicate act.

C. The RICO defendants conduct their illegal wire fraud activities and within the auspices of the app developer program and App Store organizational structure

The RICO defendants here conducted their illegal racketeering activities via a pre-existing enterprise originally established for legitimate business purposes, i.e., the highly-structured App Store hierarchy and complimentary app developer program organizational structure.

It is clear that that the overall organization constitutes an "enterprise" under the RICO statutes[38] and that each of the RICO defendants "associated" with that organization. Further, the App Store and app developer program organization enterprise maintains an ongoing, formal structure (basically, that needed and established for running its day-to-day business) separate and

---

indefinitely into the future," or "where it is shown that the predicates are a regular way of conducting defendant's ongoing legitimate business."

Word of Faith World Com. Outreach Center Church, Inc. v. Sawyer, 90 F.3d 118, 122 (5th Cir. 1996) (emphasis addedand citation omitted). "[C]riminal conduct forms a pattern if [as here] it embraces criminal acts that have the same or similar purposes, results, participants, victims, or methods of commission, or otherwise are interrelated by distinguishing characteristics and are not isolated events." 18 U.S.C. § 3575(e).

[38] For the purpose of RICO, "[a]n enterprise is a group of persons or entities associating together for the common purpose of engaging in a course of conduct . . . [;] [t]he enterprise may be a legal entity or 'any union or group of individuals associated in fact although not a legal entity.'" *Whelan v. Winchester Production Co*., 319 F.3d 225, 229 (5th Cir. 2003) (quoting 18 U.S.C. § 1961(4) and citing *U.S. v. Turkette*, 452 U.S. 576, 593, 101 S.Ct. 2524, 2528 (1981)); *United States v. Elliot*, 571 F.2d 880 (5th Cir. 1978, reh'g en banc denied) ("'Congress gave the term 'enterprise' a very broad meaning". On its face and in light of its legislative history, the Act clearly encompasses "not only legitimate businesses but also enterprises which are from their inception organized for illicit purposes". . . There is no distinction, for "enterprise" purposes, between a duly formed corporation that elects officers and holds annual meetings and an amoeba-like infra-structure that controls a secret criminal network.") (quoting *United States v. Hawes*, 529 F.2d 472, 479 (5th Cir. 1976) and *United States v. McLaurin*, 557 F.2d 1064, 1073 (5th Cir. 1977)). The element of "enterprise" required to support a RICO claim is proved by evidence of an ongoing organization, formal or informal, and by evidence that the associates function as a continuing unit. *See Boyle v. U.S*., 129 S.Ct. 2237 (2009).

apart from the pattern of racketeering activity (i.e., the spyware distribution/activation and resultant illegal acquisition of iDevice address book properties).[39]

Apple's role in creating and releasing co-defendants' address-book-poaching apps was, according to its own statements, more than just not minding the App Store. SAC ¶¶ 98, 110-11, 133-35, 410-14. These apps incorporate Apple guidance and include Apple components and certificates. SAC ¶¶ 102-03, 112. As alleged in the SAC, Apple repeatedly worked actively with its co-defendants to knowingly make, put out, and distribute to a network of iDevices via the App Store hierarchy these faulty, harmful, noncompliant address-book-poaching app products. SAC ¶¶ 103, 106, 133-35, 142-45.

Apple did not merely unwittingly assist the poachers; in view of its admissions it conspired with them,[40] SAC ¶¶ 133-35, 142-45, received business benefits from placing these apps on millions of consumers' iDevices, SAC ¶¶ 133-5, 361-68, and continues to provide cover for them to this day.[41] SAC ¶¶ 3, 4, 67, 71-72. Apple and each of its RICO co-defendants, it appears, joined to form a spyware distribution/address book contacts acquisition ring of their own, SAC ¶¶ 7, 58, 75, 102-03., 112, 114, 133-35, 362-65; *supra* nn. 18-19, 22, wherein Apple

[39] *See United States v. Turkette*, 452 U.S. 576, 583, 101 S.Ct. 2524 (1981).

[40] *Id.* Did twelve different sophisticated tech companies independently sneak apps past Apple's "comprehensive review" to simultaneously embark on schemes to poach iDevice address books using the wires? More plausible (and reasonably inferable) is that Apple green-lighted this conduct. *See supra*. These pled facts and reasonable inferences, alone, should permit Plaintiffs to move forward and discover from Defendants who knew what and when, even on claims going to the defendants' more egregiously conduct. Moreover, Apple appears to have an ownership stake in co-defendant Path, Inc. and played a hands-on advisory role in the creation of the Path app through its participation in the iFund venture fund and mentoring program. SAC ¶¶ 168. That, too, is a basis for reasonably inferring knowledge.

[41] As noted, a $99 payment ($50M annually in the aggregate to Apple) for participation in Apple's iOS developer program is apparently all it takes for an app company to come within Apple's self-imposed, ongoing sphere of protection from consumer claims about harmful apps. SAC ¶¶ 98; *compare, e.g.,* Apple's IDPLA [Dkt # 134-6] at p. 7 § 3.3.6 (supposedly prohibiting apps that "record" owners' iDevice data without notice or consent or violate private laws) *with* Apple's Motion to Dismiss [# 147] at pp. 2 and 16-17 (asserting now on the app companies' behalf that consumers cannot sue them for taking and using their address books, irrespective of how the address books were procured and whether consensual or not).

and the RICO Group II[42] co-defendants collaboratively and repeatedly used the wires and the internet[43] (i.e., a network), *e.g.,* SAC ¶¶ 175, 357-59, 391-404, and the networked on- and off-device App Store hierarchy (another network/enterprise), SAC ¶¶ 86, 93-99, 106, 197, 205, 215, 225, 231, 238, 246-47, to distribute Trojan-horse malware to millions of networked iDevices, turning recipients' iDevices into prohibited bots[44] which, in essence, electronically eavesdropped on their owners and (again via the internet and the airwaves) disclosed their associates to others and took and reported back to each respective co-defendant the iDevice owners' private, proprietary address books, SAC ¶¶ 56-59, 80, 186, 200, 208, 219-20, 228, 235, 240, 249, 253, 264, which defendants then used and integrated without consent into their own networks.[45] Accordingly, Plaintiffs state a valid RICO claim as to Apple. SAC ¶¶ 79, 156, 162, 186, 201, 208, 220, 228, 236, 240, 249,-51, 265-66, 418-420, 425, 427.[46]

[42] RICO Group I is discussed in Plaintiffs' Response to the Apple's co-defendants Rule 12(b)(6) motion to dismiss.
[43] *See United States v. Faulkner*, 17 F.3d 745, 771 (5th Cir. 1994) (noting the essential elements of wire fraud to be: (1) a scheme to defraud and (2) the use of, or causing the use of, interstate wire communications to execute the scheme), *cert. denied*, 115 S.Ct. 193 (1995).
[44] TEX. BUS. COM. CODE § 324.054-.055 (prohibiting spyware, computer "bots" or "zombies," and unauthorized use of another's computer or transmission of another's computer data).
[45] *See, e.g., U.S. v. Elliot*, 571 F.2d 880 (5th Cir. 1978, reh'g en banc denied) ("Here, the government proved beyond a reasonable doubt the existence of an enterprise comprised of at least five of the defendants. This enterprise can best be analogized to a large business conglomerate. Metaphorically speaking, J. C. Hawkins was the chairman of the board, functioning as the chief executive officer and overseeing the operations of many separate branches of the corporation. An executive committee in charge of the "Counterfeit Title, Stolen Car, and Amphetamine Sales Department" was comprised of J. C., Delph, and Taylor, who supervised the operations of lower level employees such as Farr, the printer, and Green, Boyd, and Jackson, the car thieves. Another executive committee, comprised of J. C., Recea and Foster, controlled the "Thefts From Interstate Commerce Department", arranging the purchase, concealment, and distribution of such commodities as meat, dairy products, "Career Club" shirts, and heavy construction equipment. An offshoot of this department handled subsidiary activities, such as murder and obstruction of justice, intended to facilitate the smooth operation of its primary activities. Each member of the conglomerate, with the exception of Foster, was responsible for procuring and wholesaling whatever narcotics could be obtained. The thread tying all of these departments, activities, and individuals together was the desire to make money.").
[46] Defendants Rovio and ZeptoLab, who collaborated with Chillingo to make integrated app products (i.e. RICO Group I) that poach address books, each also formed their own sub-conspiracies between themselves and Chillingo.

C. Plaintiffs state a valid aiding and abetting claim against Apple.

Apple contends that the tort of "aiding and abetting" is not recognized in Texas and, consequently and erroneously, it cannot be subject to joint liability for materially assisting (even knowingly) in its co-defendants' conduct. Apple's focus on nomenclature is misplaced. While "aiding and abetting" liability as the identification of a tort is admittedly not settled in Texas, courts routinely assess liability on claims brought under concert of action or substantial assistance theories.[47] Plaintiffs' claims against Apple pertaining to its actions with its co-defendants satisfy both theories.

Substantial assistance merely requires that Apple must know that the primary actor (here each of the Application Defendants) is breaching a legal duty and Apple's awareness of, and "substantial assistance and encouragement" to, the defendants to carry out this act. *Id.* at *9. (Liability for common design or concert-of-action differs slightly only in that it requires the aider and abetter, Apple, to have specific intent or be grossly negligent by helping the primary actor (each of the defendants App Developers) accomplish an unlawful purpose. *Id.)*

Under either theory, for the reasons espoused in the RICO section as well, Plaintiffs state a claim. In fact, Plaintiffs have alleged that Apple claimed to have "rigorously reviewed" each app and , accordingly per the reasonable inference, knew it these co-defendants' apps were essentially malware that would take Plaintiffs' private iDevice address books without their asking permission. SAC ¶¶ 277-281, 154-156. Under Texas Penal Code §33.02 or California Penal Code §502, this constitutes a crime as well as an intentional invasion of privacy, theft of trade secrets and a host of torts. *See generally* SAC.

Apple also knew that the defendants' apps secretly took iDevice address books without permission and knew, therefore, that the defendants were engaged in criminal and tortious

[47] *C.W. Zirus,* 2012 WL 377, 6978 at *8 (W.D. Tex. Aug. 29, 2012).

conduct. SAC ¶ 416. Despite this knowledge, Apple assisted and enabled the defendants by teaching App Developers to incorporate surreptitious data harvesting functionalities to take Plaintiffs' address book contents and to design these functions to operate in a stealth like fashion, to take advantage of the security hole it purposefully kept in the iDevice. SAC ¶¶ 134-37S, 278-280, 415-420.

Based on this alleged knowledge intent (which is a fact issue that must be construed in favor of Plaintiffs) and gross negligence must be inferred as alleged – especially at the motion to dismiss stage. Under Restatement 876 and *Juhl v. Airington*, 936 S.W. 2d 640, 643 (Tex. 1996), this is sufficient to show substantial assistance.[48] Here, the nature of the wrongful act alleged amounts to a crime under Texas or California Law and Apple instructed defendants, enabled their Apps, and delivered the app that did this, Apple knew this was occurring, Plaintiffs pled a viable concert of action and encouraging claim as to Apple. Essentially, Apple and the defendants worked together to infect Plaintiffs iDevices with spyware and knew they were committing crimes and torts, however minor Apple wishes to characterize them. Accordingly, provided the Court allows Plaintiffs to proceed on the underlying claims against the App Developer Defendants, the Court should not dismiss their aiding and abetting claim against Apple.

D. Plaintiffs state a valid negligence claim against Apple.

As the Court is well aware, the elements of negligence are duty and damages proximately caused by the breach. *El Chico Corp. v. Poole*, 732 S.W. 2d 306, 311 (Tex. 1987). Likewise, it is

[48] Courts generally consider five factors when assessing substantial assistance: (1) the nature of the act; (2) the kind and amount of assistance; (3) the relation of the defendant and the actor; (4) the presence or absence of the defendant at the occurrence of the wrongful act; and (5) the defendants' state of mind. *Restatement* 876; *Juhl* 936. S.W. 2d at 643. When balanced, these factor favor Plaintiffs. Working in concert, Apple instructed defendants on exploiting their flawed design, actually activated the App so that it could be provided to its consumer base, and knowingly helped the defendants place spyware on Plaintiffs' iDevice in violation of computer crime statutes.

well settled that once a party voluntarily assumes a duty, that the party must exercise reasonable care to fulfill it. *Bolin v. Tenneco Oil Co.*, 373 S.W. 2d 350 (Tex. Civ. App. – Corpus Christi 1963, writ ref'd n.r.e). In this matter, Plaintiffs SAC alleges Apple assumed a duty – not based on hidden agreements, but based on public assertions and statements to protect users' privacy from third party apps, malware or harmful code and in compliance with industry standards that they and their competitors created. SAC ¶¶ 118.

Apple has publicly represented that apps from the App Store and may and will not have hidden features that take users' personal information without permission. SAC ¶¶ 118-120. Steve Jobs, Apples' then CEO, publicly stated that the App Store would not distribute Apps that steal user's private data (such as one's iDevice address book). SAC ¶¶ 124-127. And Apple's guidelines and agreements with App Developers, which are hardly private, purport to preclude malware and the taking without consent of address book contents. SAC ¶¶ 98-129. Combined with Apple's acknowledgement that the address book database is owned by the user, that Apps were sandboxed, and malware prohibited, Apple clearly assumed a duty to protect its users' privacy that conflicts with any purported disclaimer that it might attempt to bury in an indecipherable, 37-page set of purported terms. SAC ¶¶ 124-134. In fact, as alleged in the SAC, Apple represented to the FCC that it engaged in a "rigorous review" process of all apps in order to protect their consumers' privacy. It should not be permitted to represent to the government it is protecting consumers' privacy by reviewing apps for privacy and then disclaim that duty through a web based privacy policy. Furthermore, Apple, through then CEO Steve Jobs, publically expressed that he considered the address book was protected from incursion, *i.e.* sandboxed, and that the address book was private and owned by its user. ¶¶ 116-129.

As Plaintiffs alleged that Apple breached this duty and that the breach caused Plaintiffs to suffer damage to their property (i.e., infection of spyware, impaired performance, the need for inspection and repair, use of data time, and theft of their property), Plaintiffs' negligence claim should not be dismissed.

As far as whether Apple sufficiently disclaimed this duty (and its statements suggest otherwise), this issue is not proper grounds for dismissal at this time. Not only are the documents submitted by Apple outside the pleadings, Apple expressly assumed a duty to protect its users in this fashion. The law is clear that a party may be liable for failure to protect someone from a known harm and that a duty of reasonable care exists when in general, reasonable men and women would recognize it and agree that it exists. *Otis Eng'g Corp. v. Clark*, 668 S.W. 2d 307, 310 (Tex. 1983); *Missouri, K & T. RR. Co. of Texas v. Wood,* 66 S.W. 449 (1902). Here, the risks of harm were known and foreseeable, and well certain. Apple knew and even participated in the wrongdoing. Thus, knowingly failing to protect its customers from malware that takes iDevice address book materials without a user's consent was negligent. *See, e.g*., *Wilson v. Brister*, 982 S.W 2d 42 (Tex. App. – Houston [1st Dist.] 1998, writ denied). Thus, landowners and businesses owe to invitees and customers to protect them from the criminal acts of third parties, particularly when they have in whole or in part created the circumstances that led to the criminal conduct. *Berly*, 876 S.W. 2d at 188.[49]

[49] Unlike *Doe v. MySpace,* 474 F. Supp. 2d 843, 850 (W.D. Tex. 2007), Apple played a large and direct role in the theft of Plaintiffs' address books. They knew Defendants were taking and uploading their address books, they had reviewed the apps and provided material assistance in terms of instruction and code, and they ran an electronic storefront. Thus, unlike the young girl who was sexually assaulted in a parking lot outside the control of MySpace, here, Plaintiffs were victimized on their iDevices with apps directly under Apple's control. And unlike the situation in MySpace, Apple was not lied to. On the contrary, Apple and the apps it was selling or otherwise providing were hiding material inform,atiomn from their customers.

As breaching each of the duties described above, and as alleged in the SAC, caused damages to Plaintiffs' property, *i.e.*, their iDevices, Apple's motions to dismiss Plaintiffs' negligence claim should be denied.

Significantly, the present case is nothing like the cases cited by Apple involving latent defects and retailers who do not know a product is defective. Here, Plaintiffs allege that Apple knew each App was defective and would operate a vehicle for address book theft (*e.g.,* SAC ¶¶ 146-150, 161) and that Apple was told by scientists that Gowalla was engaging in address book theft. Far from addressing the problem, as Apple claims it did, Apple ignored the complaint, let the matter fester for years, and continued to provide malicious, address book-stealing Apps like Gowalla and those of the rest of its co-defendants' to g consumers such as Plaintiffs. SAC ¶¶ 146-50. Based on these allegations, Apple would not even be entitled to the innocent retailer defense under Texas Civil Practices and Remedies Code §82.003 because the pleadings specifically allege that Apple knew that defendants' apps were acquiring and uploading address book information without consumers' consent. *See Supra*. Regardless, Plaintiffs' negligence claim should not be denied.

E. Plaintiffs state a viable unjust enrichment claim.

Unjust enrichment rests on a simple equitable principle: one who received benefits unjustly must make restitution for those benefits. *Villereal v. Grant Geophysical, Inc.*, 136 S.W. 3d 265, 270 (Tex. App. – San Antonio 2004, pet. denied). Despite Apple's claim to the contrary, unjust enrichment is actionable when a person wrongfully "secures a benefit or passively receives one which it would [be] unconscionable to retain." *Id.* (quoting *City of Corpus v. S.S. Smith and Sons Masonry, Inc.,* 737 S.W. 2d 247, 250 (Tex. App.–Corpus Christi 1987, writ denied). Put another way, a plaintiff may recover for unjust enrichment when a person obtains a

benefit from another by fraud, duress or the taking of undue advantage. *Heldenfels Bros., Inc. v. City of Corpus Christi*, 832 S.W. 2nd 39, 41 (Tex. 1992).

As The Texas Supreme Court and Fifth Circuit have recognized unjust enrichment claims in myriad actions, Apple properly does not challenge the existence of the claim *See. e.g., Texas Health Care/ Diagnostic Corp. v. Blue Cross, and Blue Shield of Texas*, 2012 WL 1617087 at * 7, (N.D. Tex. 2012). *citing Heldenfels Bros. v. City of Corpus Christi*, 832 S.W. 2d 39, 41 (Tex. 1992); *Elledge v. Friberg-Cooper Water Supply Corp.*, 240 S.W 3d 869, 870 (Tex. 2007); and *Sullivan v. Leor Energy, LLC,* 600 F. 3d 542, 550 (5th Cir. 2010).[50] Instead, Apple contends it received no benefit as the apps in question were "free."

The Court may dispense with this argument quickly as it is demonstrably false. First, Plaintiffs did not allege that all defendants' apps were free, so Aapple is attempting to interject new facts from outside the pleadings. Second, the SAC alleges that Apple receives monetary and non-monetary benefits. SAC 104, 168.Moreover, through Apple's actions, Apple not only failed to fairly compensate Plaintiffs for their losses and cause Plaintiffs privacy to be invaded, Apple gained market-share, grew its App Store significantly, and profited directly (i.e. 30% per download) from paid Apps like *Angry Birds* and *Cut the Rope* privacy, and Apple increased its value. SAC ¶¶ 418-422.

Further, as alleged in the SAC, Apple assisted co-efendants acquire Plaintiffs' private iDevice address book materials without Plaintiffs' consent. As alleged, these iDevice address books had commercial value, intrinsic value, and were of enormous financial benefit to Apple and its co-defendants. SAC ¶¶ 77, 314-325, 418-422. Thus, the Court should not dismiss

[50] Nor is a cause of action for unjust enrichment limited to Texas. California law also authorizes recovery o unjust enrichment, and has done so in the case Apple contends is related. *See Path v. Hernandez*, 2012 WL 5194120 at • 8 (N.D. Cal).

Plaintiffs' unjust enrichment claim. Otherwise, Apple and its co-defendants' will be rewarded for and retain the benefits of their wrongful actions.[51]

IV. Conclusion

For the foregoing reasons, Apple's motion to dismiss should be denied.

Respectfully submitted,

EDWARDS LAW

By: _____

Jeff Edwards
State Bar No. 24014406
THE BREMOND HOUSTON HOUSE
706 GUADALUPE
Austin, Texas 78701
Tel. 512-623-7727
Fax. 512-623-7729
jeff@edwards-law.com

Carl F. Schwenker
Texas Bar No. 00788374
LAW OFFICES OF CARL F. SCHWENKER
The Bremond-Houston House
706 Guadalupe Street
Austin, Texas 78701
Tel. (512) 480-8427
Fax (512) 857-1294
cfslaw@swbell.net

Dirk Jordan
Texas Bar No. 00784359
Jordan Law Firm
The Bremond-Houston House
706 Guadalupe Street
Austin, Texas 78701
512-551-0669
512-551-0668 fax
dirk@dirkjordan.com

ATTORNEYS FOR THE PLAINTIFFS
AND THE PUTATIVE CLASS

CERTIFICATE OF SERVICE

On November 12, 2012, a copy of the foregoing motion was electronically filed on the CM/ECF system, which automatically serves a Notice of Electronic Filing on the following:

Attorneys for Defendants Apple, Inc.:

Alan D. Albright
BRACEWELL & GIULIANI LLP
111 Congress Avenue, Suite 2300
Austin, Texas 78701
(512) 494-3620 – Telephone
(512) 472-9123 – Facsimile
Email: alan.albright@bgllp.com

Susan Ashlie Beringer
GIBSON, DUNN & CRUTCHER LLP
1881 Page Mill Road
Palo Alto, California 94304-1211
(650) 849-5219
(650) 849-5019

William B. Dawson
Scott Howard Mellon
GIBSON, DUNN & CRUTCHER LLP
2100 McKinney Avenue, Suite 1100
Dallas, Texas 75201
(214) 698-3132 – Telephone
(214) 571-2919 – Facsimile
Email: wdawson@gibsondunn.com;
smellon@gibsondunn.com

Attorneys for Defendants Chillingo Ltd. and Electronic Arts, Inc.:

Hal L. Sanders, Jr.
Adam Hugh Sencenbaugh
HAYNES AND BOONE, LLP
600 Congress Avenue, Suite 1300
Austin, Texas 78701
(512) 867-8427 – Telephone
(512) 867-8667 – Facsimile
Email: hal.sanders@haynesboone.com;
adam.sencenbaugh@haynesboone.com

Marc J. Zwillinger
Jacob Allen Sommer
ZWILLGEN PLLC
1705 N. St. NW
Washington, DC 20036
(202) 296-3585 – Telephone
(202)706-5298 – Facsimile
Email: marc@zwillgen.com
jake@zwillgen.com

Attorneys for Defendants Facebook, Inc., Instagram, Inc. and Kik Interactive, Inc.:

Lori R. Mason
COOLEY, LLP
5 Palo Alto Square
3000 El Camino Real
Palo Alto, California 94306
(650) 843-5000 – Telephone
(650) 849-7400 – Facsimile
Email: lmason@cooley.com

Mazda K. Antia
Michael G. Rhodes
COOLEY, LLP
4401 Eastgate Mall
San Diego, California 92121
(858) 550-6000 – Telephone
(858) 550-6420 – Facsimile
Email: mantia@cooley.com;
mrhodes@cooley.com

Attorneys for Defendants Foodspotting, Inc. and Yelp! Inc.:

Peter D. Kennedy
GRAVES, DOUGHERTY, HEARON & MOODY, PC
401 Congress Avenue, Suite 2200
Austin, Texas 78701
(512) 480-5764 – Telephone
(512) 536-9908 – Facsimile
Email: pkennedy@gdhm.com

Michael Page
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, California 94111
(415) 362-6666 – Telephone
(415) 236-6300 – Facsimile
Email: mpage@durietangri.com

Attorneys for Defendant Foursquare Labs, Inc.:

Keith Mason Henneke
MORRISON & FOERSTER LLP
555 West Fifth Street, 35th Floor
Los Angeles, California 90013
(213) 892-5200 – Telephone
(213) 892-5454 – Facsimile
Email: khenneke@mofo.com

Attorneys for Defendant Gowalla Incorporated:

Michael J. Biles
KING & SPALDING LLP
401 Congress Avenue, Suite 3200
Austin, Texas 78701
(512) 457-2000 – Telephone
(512) 457-2100 – Facsimile
Email: mbiles@kslaw.com

Daniel Weinberg
Indra Neel Chatterjee
Morvarid Metanat
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, California 94025
(650) 614-7400 – Telephone
(650) 614-7401 – Facsimile
Email: dweinberg@orrick.com;
nchatterjee@orrick.com;
mmetanat@orrick.com

M. Leah Somoano
ORRICK, HERRINGTON & SUTCLIFFE, LLP
2050 Main Street, Suite 1100
Irvine, California 92614
(949) 567-6700 – Telephone
(949) 567-6710 – Facsimile
Email: lsomoano@orrick.com

Attorneys for Defendant Path, Inc.:

Gregory J. Casas
GREENBERG TRAURIG, LLP
300 West 6th Street, Suite 2050
Austin, Texas 78701
(512) 320-7238 – Telephone
(512) 320-7210 – Facsimile
Email: casasg@gtlaw.com

Jedediah Wakefield
Tyler G. Newby
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
(415) 875-2300 – Telephone
(415) 281-1350 – Facsimile
E-mail: jwakefield@fenwick.com;
switnov@fenwick.com;
tnewby@fenwick.com

Attorneys for Defendant Rovio Mobile Oy a/k/a Rovio Entertainment Ltd.:

Shannon W. Bangle
BEATTY, BANGLE, STRAMA P.C.
400 West 15th Street, Suite 1450
Austin, Texas 78701
(512) 879-5050 – Telephone
(512) 879-5040 – Facsimile
Email: sbanble@bbsfirm.com

Christopher G. Kelly
Judith R. Nemsick
HOLLAND & KNIGHT LLP
31 West 52nd Street
New York, New York 10019
(212) 513-3200 – Telephone
(212) 385-9010 – Facsimile
Email: judith.jemsick@hklaw.com
christopher.kelly@hklaw.com

Attorneys for Defendant Twitter, Inc.:

Tanya D. Henderson
PERKINS COIE LLP
2001 Ross Avenue, Suite 4225
Dallas, Texas 75201
(214) 965-7700 – Telephone
(214) 965-7799 – Facsimile
Email: thenderson@perkinscoie.com

Timothy L. Alger
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, California 94304
(650) 838-4300 – Telephone
(650) 838-4350 – Facsimile
E-mail: talger@perkinscoie.com

Amanda J. Beane
Ryan T. Mrazik
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101
(206) 359-8000 – Telephone
(206) 359-9000 – Facsimile
E-mail: abeane@perkinscoie.com;
rmrazik@perkinscoie.com

Attorneys for Defendant ZeptoLab UK Ltd.:

Lawrence A. Waks
Emilio B. Nicolas
JACKSON WALKER L.L.P.
100 Congress Avenue, Suite 1100
Austin, Texas 78701
(512) 236-2000 – Telephone
(512) 236-2002 – Facsimile
E-mail: lwaks@jw.com; enicolas@jw.com

Christine Lepera (*pro hac vice*)
Jeffrey M. Movit (*pro hac vice*)
MITCHELL SILBERBERG & KNUPP LLP
12 East 49th Street, 30th Floor
New York, New York 10017-1028
(212) 509-3900 – Telephone
(212) 509-7239 – Facsimile
E-mail: ctl@msk.com; jmm@msk.com

By: /s/
Carl F. Schwenker